

A short proof of a known result about the density of a certain set in

$$[0, 1]^n$$

Dimitri Dias

### Abstract

In Theorem 1 of [CZ01], Cobeli and Zaharescu give a result about the distribution of the  $\mathbf{F}_p$ -points on an affine curve. An easy corollary to their theorem is that the set

$$\bigcup_p \left\{ \left( \frac{x_1}{p}, \dots, \frac{x_n}{p} \right), 1 \leq x_i < p \text{ and } \prod_{1 \leq i \leq n} x_i \equiv 1 \pmod{p} \right\}$$

is dense in  $[0, 1]^n$ . In [Foo07], Foo gives a elementary proof of that fact in dimension 2. Following Foo's ideas, we give a similar proof in dimension greater than or equal to 3.

## 1 Introduction

In Theorem 1 of [CZ01], Cobeli and Zaharescu give a result about the distribution of the  $\mathbf{F}_p$ -points on an affine curve. In dimension  $n$ , for any curve  $\mathcal{C}$  over  $\mathbb{F}_p$  not contained in any hyperplane, for any nice domain  $\Omega$  in the torus  $\mathbb{T}^n$  and for any prime  $p$ , let  $\mu$  be the normalized Haar measure on  $\mathbb{T}^n$  and  $\mu_{n,p,\mathcal{C}} = \frac{1}{|\mathcal{C}(\mathbb{F}_p)|} \sum_{x \in \mathcal{C}(\mathbb{F}_p)} \delta_{t(x)}$ , with  $\delta_{t(x)}$  a unit point delta mass at  $t(x)$ , where  $t$  is a natural injection from  $\mathbb{F}_p^n$  to  $\mathbb{T}^n$ . Cobeli and Zaharescu quantify how fast  $\mu_{n,p,\mathcal{C}}(\Omega)$  approaches  $\mu(\Omega)$  and their result easily imply that the set

$$\mathcal{A}_n = \bigcup_p \left\{ \left( \frac{x_1}{p}, \dots, \frac{x_n}{p} \right), 1 \leq x_i < p \text{ and } \prod_{1 \leq i \leq n} x_i \equiv 1 \pmod{p} \right\}$$

is dense in  $[0, 1]^n$ .

Their proof mainly uses exponential sums and, as remarked by Foo in [Foo07], one can give an elementary proof of the previous fact in dimension 2. Following his ideas, we prove the result in dimension greater than or equal to 3.

**Theorem 1.** *Let  $n \geq 3$ . The set  $\mathcal{A}_n$  is dense in  $[0, 1]^n$ .*

## Acknowledgements

I would like to thank my supervisor, Professor Andrew Granville, for discussions that greatly helped me with my work. I would also like to thank my friends Marc Munsch, Oleksiy Klurman, Crystel Bujold and Marzieh Mehdizadeh for their helpful comments.

## 2 Proof of Theorem 1

We will need the following lemmas:

**Lemma 1.** *Let  $x \in [0, 1]$  and  $0 < \varepsilon \leq 1$ . Let  $N$  such that  $N > \frac{1}{\varepsilon}$  and  $c_3 \frac{(\log N)^{c_2}}{N} < \frac{\varepsilon}{2}$  (where  $c_2$  and  $c_3$  are absolute constants defined in the proof). Then, for every  $b \geq N$ , there exists  $1 \leq a < b$  with  $(a, b) = 1$ ,  $a > \frac{\varepsilon}{2}b$  and  $|x - \frac{a}{b}| < \varepsilon$ .*

*Proof.* Let  $b \geq N$  and consider the set

$$\mathcal{D}_b = \left\{ \frac{a}{b} \text{ with } 1 \leq a < b \text{ and } (a, b) = 1 \right\}.$$

Let  $g(b)$  be the least integer such that every set of  $g(b)$  consecutive integers contains at least one integer relatively prime to  $b$ . As remarked by Erdős in [Erd62], a standard application of Brun's method gives that

$$g(b) \leq c_1 \omega(b)^{c_2}$$

where  $\omega(b)$  denotes the number of prime factors of  $b$  and  $c_1, c_2$  are absolute constants. Therefore, the distance between two consecutive elements of  $\mathcal{D}_b$  is bounded above by

$$\frac{g(b)+1}{b} \leq \frac{c_1 \omega(b)^{c_2} + 1}{b} \leq c_3 \frac{(\log b)^{c_2}}{b} < \frac{\varepsilon}{2}.$$

The minimal value of this set is  $\frac{1}{b} < \varepsilon$  and the maximal value is  $1 - \frac{1}{b} > 1 - \varepsilon$ . Therefore, for any  $x \in [0, 1]$ , there exists  $\frac{a}{b} \in \mathcal{D}_b$  with  $\frac{a}{b} > \frac{\varepsilon}{2}$  and  $|x - \frac{a}{b}| < \varepsilon$ .  $\square$

**Lemma 2.** *The set*

$$\mathcal{B}_n = \left\{ \left( \frac{a_0}{a_1}, \dots, \frac{a_{n-1}}{a_n} \right), 1 \leq a_i < a_{i+1}, (a_i, a_{i+1}) = 1 \text{ and } (a_1, a_2 \dots a_n) = 1 \right\}$$

*is dense in  $[0, 1]^n$ .*

*Proof.* Let  $(x_1, \dots, x_n) \in [0, 1]^n$  and  $\varepsilon > 0$ . We can also assume  $\varepsilon \leq 1$ . Let  $M$  such that  $c_3 \frac{\log^{c_2} M}{M} < \left(\frac{\varepsilon}{2}\right)^{n-1} \frac{1}{n^{c_2}}$  and  $M > \frac{4}{\varepsilon}$  (note in particular that  $M$  can be supposed larger than the  $N$  in Lemma 1).

Choose  $a_{n-1}$  a prime number such that  $a_{n-1} \geq \left(\frac{2}{\varepsilon}\right)^{n-2} M$ . Let

$$\mathcal{H}_{a_{n-1}} = \left\{ \frac{a_{n-1}}{m} \text{ with } a_{n-1} < m \text{ and } (a_{n-1}, m) = 1 \right\}.$$

Since  $a_{n-1}$  is prime, if  $(a_{n-1}, m) = 1$ , then either  $(a_{n-1}, m+1) = 1$  or  $(a_{n-1}, m+2) = 1$ . Therefore, the distance between two consecutive elements in the set  $\mathcal{H}_{a_{n-1}}$  is bounded above by

$$\frac{2}{a_{n-1}} < \frac{\varepsilon}{2}.$$

The set  $\mathcal{H}_{a_{n-1}}$  contains arbitrarily small elements and has maximum  $1 - \frac{1}{a_{n-1}} > 1 - \varepsilon$ . Therefore, there exists  $a_n$  such that  $(a_{n-1}, a_n) = 1$ ,  $\frac{a_{n-1}}{a_n} > \frac{\varepsilon}{2}$  and  $|x_n - \frac{a_{n-1}}{a_n}| < \varepsilon$  (we will need  $a_n$  not too large in terms of  $a_{n-1}$  in Equation 1).

Using Lemma 1 ( $n-3$ ) times, we find  $a_{n-2}, \dots, a_2$  with  $(a_i, a_{i+1}) = 1$ ,  $a_i > \frac{\varepsilon}{2} a_{i+1}$  and  $|x_i - \frac{a_{i-1}}{a_i}| < \varepsilon$  (the choice of  $a_{n-1}$  large enough in terms of  $M$  allows us to apply Lemma 1 at each step).

To find  $a_1$ , we need a slightly modified version of Lemma 1. Let

$$\mathcal{D}_{a_2} = \left\{ \frac{m}{a_2} \text{ with } 1 \leq m < a_2 \text{ and } (m, a_2 \dots a_n) = 1 \right\}.$$

The difference between two consecutive elements in this set is bounded by

$$(1) \quad \frac{g(a_2 \dots a_n) + 1}{a_2} \leq c_3 \frac{\log^{c_2}(a_2 \dots a_n)}{a_2} \leq c_3 \left(\frac{2}{\varepsilon}\right)^{n-3} \frac{\log^{c_2}\left(\left(\frac{2}{\varepsilon}\right) a_{n-1}^{n-1}\right)}{a_{n-1}} < \frac{\varepsilon}{2}$$

from our choice of  $M$ . The minimal value of this set is  $\frac{1}{a_2} < \varepsilon$ , and if we derestrict  $m$  and let it go to infinity, we cover all of  $[0, +\infty)$  with intervals of length at most  $\frac{\varepsilon}{2}$ . Therefore, one can always find  $\frac{a_1}{a_2} \in \mathcal{D}_{a_2}$  such that  $\left|x_2 - \frac{a_1}{a_2}\right| < \varepsilon$  and  $\frac{a_1}{a_2} > \frac{\varepsilon}{2}$ .

To find  $a_0$ , one can simply apply Lemma 1 again.  $\square$

For the sake of completeness, we re-prove the following lemma of [Foo07], which suffices to prove Theorem 1.

**Lemma 3.** *The set  $\mathcal{A}_n$  is dense in the set  $\mathcal{B}_n$ .*

*Proof.* Let  $\left(\frac{a_0}{a_1}, \dots, \frac{a_{n-1}}{a_n}\right) \in \mathcal{B}_n$ . Consider the sequence (which exists, as a consequence of Dirichlet's theorem)

$$\left(\frac{a_0 p + a_n}{p a_1}, \dots, \frac{a_{n-1}(p+1)}{p a_n}\right)_p \text{ with } p \equiv -a_0^{-1} a_n \pmod{a_1} \text{ and } p \equiv -1 \pmod{a_2 \dots a_n}.$$

Then, this sequence is in  $\mathcal{A}$  and converges to  $\left(\frac{a_0}{a_1}, \dots, \frac{a_{n-1}}{a_n}\right)$ .  $\square$

*Proof of Theorem 1.* It's a straightforward consequence of Lemma 2 and Lemma 3.  $\square$

**Remark 1 :** Using Theorem 1, one can easily prove the following slightly more general result:

**Corollary 1.** *Let  $f$  be a monic polynomial of degree  $d$ . Then, the set*

$$\bigcup_p \left\{ \left( \frac{f(x_1)}{p^d}, \dots, \frac{f(x_n)}{p^d} \right), 1 \leq x_i < p \text{ and } \prod_{1 \leq i \leq n} x_i \equiv 1 \pmod{p} \right\}$$

*is dense in  $[0, 1]^n$ .*

*Proof.* Let  $\|f\|$  be the absolute value of the largest coefficient of  $f$ . Let  $(\alpha_1, \dots, \alpha_n) \in [0, 1]^n$  and  $\varepsilon > 0$ . We can assume that  $\varepsilon \leq 1$ . Using Theorem 1, there exist  $p > \frac{2d\|f\|}{\varepsilon}$  and  $1 \leq x_i < p$  such that

$$\left| \frac{x_i}{p} - \alpha_i^{\frac{1}{d}} \right| < \frac{\varepsilon}{2^{d+1}} \quad \forall 1 \leq i \leq n \text{ and } \prod_{1 \leq i \leq n} x_i \equiv 1 \pmod{p}.$$

Therefore,

$$\left| \frac{x_i^d}{p^d} - \alpha_i \right| < \sum_{k=0}^{d-1} \binom{d}{k} \left( \frac{\varepsilon}{2^{d+1}} \right)^{d-k} < \frac{\varepsilon}{2} \quad \forall 1 \leq i \leq n$$

and

$$\left| \frac{f(x_i)}{p^d} - \frac{x_i^d}{p^d} \right| \leq \frac{\|f\|}{p^d} \sum_{k=0}^{d-1} |x_i|^k \leq \frac{d\|f\|}{p} < \frac{\varepsilon}{2} \quad \forall 1 \leq i \leq n.$$

This suffices to prove the result.  $\square$

**Remark 2 :** The theorem of [CZ01] implies that a statement similar to Theorem 1 is true for a whole family of curves. It would be interesting to see if the previous elementary proof can be extended to curves other than  $\prod_{1 \leq i \leq n} x_i \equiv 1 \pmod{p}$ .

## References

- [CZ01] Cristian Cobeli and Alexandru Zaharescu. On the distribution of the  $\mathbf{F}_p$ -points on an affine curve in  $r$  dimensions. *Acta Arith.*, 99(4):321–329, 2001.
- [Erd62] P. Erdős. On the integers relatively prime to  $n$  and on a number-theoretic function considered by Jacobsthal. *Math. Scand.*, 10:163–170, 1962.
- [Foo07] Timothy Foo. A short proof of a known density result. *Integers*, 7:A7, 3, 2007.

DÉPARTEMENT DE MATHÉMATIQUES ET STATISTIQUES, UNIVERSITÉ DE MONTRÉAL, CP 6128 SUCC. CENTRE-VILLE,  
MONTRÉAL QC H3C 3J7, CANADA

*Email address:* `dimitrid@dms.umontreal.ca`